CONFIDENTIAL REPORT A52

SURVEILLANCE SECRETS

By

Jack Crawford

NIGHT SKY

NIGHT SKY - CONFIDENTIAL REPORT A52

SURVEILLANCE SECRETS

by
Jack Crawford

About the Author:
Jack Crawford *has worked in law enforcement and surveillance for twentyfive years and has written two books on the subject. He currently divides his time between London and Dallas, Texas where he is a partner in a success private detective agency.*

We hope you enjoy reading this special report At NIGHT SKY LTD. our motto is Knowledge is Power. We publish useful and often difficult to obtain information, written in a clear and easy to follow format by experts in their fields. Information that will help you develop your skills and abilities and so improve your lifestyle whether on a business, educational, or a personal level.

Published By:
Night Sky Ltd
PO Box 115, St Helier JE4 8QQ

Copyright © NIGHT SKY LTD 1988
Printed and Bound in Great Britain

All rights reserved. Except for use in a review, no portion of this book may be reproduced in any form without the express written permission of the publisher. Although every effort has been made to ensure that the information given in this book is correct and accurate, neither the author nor the publisher can accept liability for any errors or omissions

Conditions of Supply

This document is a confidential report and is supplied for the use and benefit of the recipient only. No part of this document may be reproduced in any form without prior written permission from the publisher.

ISBN 1 902312 058

A Note From The Publisher

Dear Reader,

I thank you for purchasing this NIGHT SKY book and hope that you find the information it contains to be useful to you. Our aim is to publish well written information that can genuinely improve your life.

Unlike many publishers who pad out their books, at NIGHT SKY we avoid wasting words and pages and keep to the point. This enables you to read our books much faster and with greater ease, so making it easier to assimilate and benefit from the information contained.

If you have any comments or criticisms about this book, or any others that we publish, please write to me at the address below. I personally read and reply to all such letters.

Best wishes,

Bob Jardine, Publisher

Night Sky Ltd
PO Box 115, St Helier JE4 8QQ

P.S. Write to us for details of our full range of publications. We will be happy to post you our latest catalogue of exciting life changing titles – free of charge!

CONTENTS

CHAPTER ONE	*Big Brother is Watching you ...*
CHAPTER TWO	*Telephone Tapping*
CHAPTER THREE	*Cracking the Computer!*
CHAPTER FOUR	*Video Surveillance*
CHAPTER FIVE	*Classic Bug*
CHAPTER SIX	*Countersurveillance Tips & Tricks*
CHAPTER SEVEN	*Selecting the Countersurveillance Person Right For You*
CHAPTER EIGHT	*Legalities and Privacy Laws*
CHAPTER NINE	*Contact List Directory*

CHAPTER ONE

BIG BROTHER'S WATCHING YOU ...!

Just prior to this book going to press, a European Commission report warned that the United States has developed an extensive spying network on European citizens and that we should all be worried.

In brief. A global electronic spy network that can eavesdrop on every telephone, e-mail and telex communication round the world will be officially acknowledged for the first time in a European Commission report to be called *Assessing the Technologies of Political Control* and which was commissioned in 1998 by the Civil Liberties Committee of the European Parliament.

This document contains details of a network of American-controlled spy stations on British soil and around the world, that "routinely" and indiscriminately monitor countless phone, fax and e-mail messages.

It states: "Within Europe, all e-mail telephone and fax communications are routinely intercepted by the United States National Security Agency transferring all target information from the European mainland via the strategic hub of London then by satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in Yorkshire."

Plus, the report confirms, for the first time, the existence of the secretive Echelon system.

Until now, evidence of such astounding technology has been patchy and anecdotal, but this report finally confirms that the citizens of Britain and other European states are subject to an intensity of surveillance far in excess of that imagined by most parliaments.

The Echelon system forms part of the UK/USE system but, unlike many of the electronic spy systems developed during the Cold War. Echelon is designed primarily for non-military targets: governments, organisations and businesses in virtually every country.

This system works by indiscriminately intercepting very large quantities of communications and then siphoning out what is valuable using artificial intelligence aids like MEMEX to find key words.

According to the report, Echelon uses a number of national dictionaries containing key words of interest to each country.

For more than a decade, former agents of US, British, Canadian and New Zealand national security agencies have claimed that the monitoring of electronic communications has become endemic throughout the world. Rumours have circulated that new technologies have been developed which have the capabilities to search most for the world's telex, fax and e-mail networks for key words. Phone calls, they claim, can be automatically analysed for key words.

Former signals intelligence operatives have similarly stated that spy bases controlled by America have the ability to search nearly all data communications in the same way. They claim that Echelon automatically analyses most e-mail messages for 'precursor' data which assists intelligence agencies to determine targets. According to former Canadian Security Establishment agent, Mike Frost, a voice recognition system called Oratory has been used for some years to intercept diplomatic calls.

Glyn For, Labour MEP for Greater Manchester believes that the report is critical to the future of civil liberties in Europe.

"In the civil liberties committee, we spend a great deal of time debating issues such as free movement, immigration and drugs. Technology always sits at the centre of these discussions. There are times in history when technology helps democratise and times when it helps centralise. This is a time of centralisation. The justice and home affairs pillar of Europe has become more powerful without a corresponding strengthening of civil liberties."

The report recommends a variety of measures for dealing with the increasing power of the technologies of surveillance being used at Menwith Hill and other centres. It bluntly advises. "The European Parliament should reject proposals from the United States for making private messages via the global communications network (Internet) accessible to US intelligence agencies."

The report also urges a fundamental review of the involvement of the American NSA (National Security Agency) in Europe, suggesting that the activities be either scaled down, or become more open and accountable.

Such concerns have been privately regressed by governments and MEP's since the Cold War, but surveillance has continued to expand US intelligence activity in

Britain and enjoyed a steady growth throughout the past two decades. The principal motivation for this rush of development is the US interest in commercial espionage. In the Fifties, during the development of the "special relationship" between America and Britain, one US institution was singled out for special attention.

The NSA, the world's biggest and most powerful signals intelligence organisation, received approval to set up a network of spy stations throughout Britain. Their role was to provide military, diplomatic and economic intelligence by intercepting communications from throughout the Northern Hemisphere.

The NSA is one of the shadowest of the shadowy US intelligence agencies and, until a few years ago, its existence was a secret and any mention of its duties are still classified. However, if you are on Internet, you can check out their Web site (www.nsa.gov.8080) and see just how much they are giving away – (not a lot methinks!)

CHAPTER TWO

TELEPHONE TAPPING

These days, simple eavesdropping on the phone is far easier than we maybe imagine. For example, like most people today you probably own a phone which offers several different functions, including conferencing, speed dialling, automatic redialling, etc.

You don't have to have an electrical engineering degree to listen in on a call made on one of these 'standard' phones. All that is required is that first, the person involved is dialled then, as soon as the phone is answered, the eavesdropped will hit the speed dial or re-dial function. Remember, the other person's number will have been already programmed so it will immediately dial his or her number. When the person answers the phone, the eavesdropped pushes the conferencing button and can then listen in to the two targets talking together.

The drawback here is that neither party actually dialled the other, however, most of the time, each will automatically assume that he was on the receiving end. In other words, if the calls are timed just right, the first caller will be going, "Hello, Hello," just as the second caller picks up the phone and the conversation proceeds as normal.

Likely candidates for this social tapping include solicitors and their clients, people about to close a business deal and (surprise surprise!), couples involved in extra marital relationships.

Still on the subject of simple home telephone, let's look at some other ways that are commonly used to 'tap' private conversations so that, if you think you are on the receiving end, you can take some preventive measures…

Firstly, remember that your home phone plugs into a wall jack and, from this, the wires terminate at a connector block. This is known as a surge protector and usually housed in plastic (modern) or metal (old style) housing which is pretty easy to prise open. The surge protector is generally mounted on the outside wall of the house.

Phone conversations are generally carried over two wires, known as a 'talk path'. These two wires start at your telephone and, ultimately, terminate at the phone company's central switchboard which could be anywhere from 100 feet to several miles away. So, next time you are talking on the phone with your next-door neighbour,

think about it. Your voice transmission hits the central switchboard, then goes out on your neighbour's wire pair all the way to his house (and vice versa). Thinking about that, may make you knock on the front door instead – and save the cost of that call!

Okay, now one of the simplest and most inexpensive methods of tapping that spouse, employee or significant other (provided you have access to his/her residential or office premises) is to place an automatic tape starter (which turns of the tape recorder when the phone is picked up and shuts off at the end of the conversation) and a tape recorder behind or underneath a heavy, large piece of furniture – that also just happens to have a telephone jack behind it. All that is required here is to simply cut off the modular end of the automatic tape starter, attach alligator clips and hook them anywhere across the phone line.

Think you are on the receiving end? Then, consider investing in a voltage spreader, a device that is very effective in thwarting this kind of phone tapping which retains the voltage at or above 20 volts directs current and prevents the automatic tape starter from turning on. However, these voltage spreaders will not function against voice-activated or radio frequency-type taps. So you need to know exactly what you are up against first.

The latter can be constructed by any third-rate hobbyist for less than ten pounds and can be placed anywhere along the telephone line. This means that the eavesdropper doesn't have to have his target's front key in his possession.

So, how does it work?

Simple. The radio frequency taps have a typical range of one to two blocks and broadcast both sides of the phone conversation to any "tabletop" FM radio. This is then connected to a signal-activated switch and, next, to a tape recorder. It's hard to do much to block this if you are the victim. In fact, not even those American heavies – the CIA can apparently detect it on the line.

Also, when the radio frequency tap is in place, it can be used in a car, complete with signal-activated switch and tape recorder, provided the vehicle is parked relatively closely to the building targeted. The operatives don't even have to worry if the radio frequency tap is discovered as it is no more than a tiny FM broadcast transmitter and there is no direct connection to the listening post.

While we are on the delicate subject of the US government, while researching this book (yes, on both sides of the Atlantic!) I asked several professional government employees and surveillance personnel if, indeed, every single phone in the United States is tapped.

Naturally, it was difficult to get a straight answer but, finally, one repondent explained it this way: "Microwaves may travel in a straight line, but the signal spreads out quite a bit before the receiving antenna and it is a simple matter to pick up this scatter. Most calls made in the US travel least part of their journey via microwave links or satellites." The last sentence was particularly telling I thought: "It should not be assumed that these calls couldn't be monitored."

Very interesting.

Here is one method that can be employed by so called law enforcement personnel or just those people with plenty of resources. The operatives rent what is known as a 'listening post' somewhere downwire between the target and the central switchboard. This could be any building, from an empty garage to a studio flat - as long as there's a phone line, of course.

If the utilities are above ground, the metal box containing the connector blocks is opened up. They will then do what is known as a 'bridge job' - which has nothing to do with dentistry but is rather the process of jumpering the wire pair with a listening post wire pair. All they need to do next is relax in a nice comfy chair and listen to the ensuing telephone conversation with ease – with a tape recorder at hand, of course – for all those incriminating details.

The off-premises tapping of telephone phones is not much different from tapping those at home, although there are some differences as far as inside wiring and actual installation is concerned.

Office phone systems are generally driven by a device know as a "key system unit" which mounts on the wall of a phone closet. With larger systems, it will normally be free standing and referred to, somewhat incongruously, as a 'switch'.

In the typical phone closet you will find a veritable rat's nest of wires, connector blocks and several key system units; probably one for each company that occupies a particular floor. In layman's terms, the key system unit is an electronic

microprocessor-based controller that allows employees to transfer calls, put people on hold, carry on conference calls, play dreadful music, and so on.

And all our Bond character need have to tap into this intricate electronic system is a boring old screwdriver! By donning the right colour jacket, for example, he can pretend that he is with a private telecommunications company or investigating some repair or other. An honest face will probably help, but most probably he won't be questioned.

All he needs to do then is a bridging tap which, in office buildings is often done in the splice cabinet at what is know as a 66 block. This block uses V-shaped terminals to connect the drop wires to the phone lines. A pro will use a telco seating wrench (about £8) to seat his bridge wiring so it will go unnoticed by anyone except the most dedicated searcher, or pull the block forward and attach his wire to the back of the 66 post, running it out of the block and allowing a remote installation of the listening equipment.

Cordless Telephones

Cordless telephones are a synch to intercept by the typical scanner enthusiast. And, guess what? - scanning is a popular hobby throughout the UK. At the same time, cordless phones are thankfully fast being replaced by the cellular option - which we shall come to next…

Most cordless phone users are unwittingly probably always within the range of several scanner owners. Even the cheapest police scanners have the ability to intercept cordless phone conversations and, what is more, can hear both parties equally clearly from several thousand feet away.

Interestingly, the frequency of cordless phones was published widely before most of the cordless phones ever hit the market place. This meant that millions of people with scanners, particularly in the US, had these same frequencies programmed into their scanners back in the early to mid 1980's. Although there are a growing number of cordless phones that claim to be scrambled - beware! Many of the so-called scrambled phones use techniques that are easily cracked with cheap equipment. Also if a scrambled cordless phone uses any kind of 'phase inversion techniques, it's no good. If it uses digital encryption, it's probably all right, but bear in mind that wire tappers can always tap the phone line and easily bypass your scrambled cordless phone.

A final word of caution here, anybody can use cordless phone conversations against you in a law court - at the time of writing, no special warrant was required.

Mobile Phones

In a recently released book, top thriller writer, Tom Clancy based much of the tension of his plot on the apparent fact that the government agents couldn't follow the bad guys as their mobile (cellular) phones were "impossible to monitor." Clancy really did a lousy job on his research here. I'm surprised.

On the contrary, mobile phones are probably the easiest type of communication to monitor without investing in expensive equipment but by using a halfway decent scanner. Cell phones operate in the 800 MHz frequency range but obviously change frequencies often when a person is (upwardly) mobile. This is because the person is moving into another cell location. There are countless frequencies in a typical cell phone system which means that in a large city like Manchester or Bristol there may be literally hundreds of cell phone conversations taking place at once with the same metro cell system. It is obviously far easier therefore to 'tap' in when in a small town!

Computer-aided scanning is an ideal solution here. If an operative has a good scanner with computer interface capabilities, all is not lost. Along with a black box, called a DDI (digital data interpreter) and the correct software, he or she can intercept a mobile phone conversation and follow the call with ease.

But why tap mobiles? When, at first glance, it seems to be an oxymoron. I mean why tap a cellular when it is broadcast over the public airwaves with 600 millowatts of power?

Some people want to tap everything and anything, that's why!

In this case, the fastest method to hear at least one side of any conversation is simply to secrete a voice activated tape recorder in the car. This could make a nice gift for your spouse, perhaps. There is also a handy gadget made by Olympus Corporation in the USA (see the directory at the back of the book) which is a series of drop out recorders for mobile phones. These tiny boxes connect between the handset and the phone and record both sides of the conversation when the phone is taken off the hook.

And then there is the bug that can be concealed in a rechargeable Motorola-type battery for portable phones. This unit works off the battery, which still operates the phone while, at the same time picks up and transmits local conversations.

You can even record a cellular conversation that you are part of without altering anyone else in the car. This is done via what is known as an 'ear mike' - a device that receives and transmits inside the user's ear and looks just like a miniature earphone, put one in your ear and have a conversation. That easy!

A mobile phone can also be intentionally left on after a call is made to a recording phone which means, for instance, if it is left behind during a business conference, it will work as a convenient long distance bug. Some 'smart' mobiles are now made with a hot switch so they can broadcast to a nearby receiver for the same sort of 'forgetful' bugging.

And digital phones? According to a recent report released by two US researchers the GSM digital telephone standard which is used by more than 70 million European mobile telephones (including those from Cellnet and Vodafone) was, until recently billed as the most secure mobile phone today. In fact, its encoding algorithms have been deliberately weakened.

Each GSM phone contains a smartcard that generates a 64-bit code carrying subscriber and accountant information for the service provider. Two researchers from the University of California at Berkeley cracked a GSM smartcard and found that the COMP128 algorithm invariably generates 10 zeros, at the end of the code, making a *de facto* 54-bit key. Such a code is 1,024 times easier to crack than a 64-bit key.

David Wagner, one of the researchers, said the zeros were no accident. "It doesn't speed up transmission or prolong battery life either, the only reason I can see is to help surveillance."

He and his partner, Ian Goldberg, have made it their mission to crack so-called unbreakable codes whose design process is secret. Their biggest coup cam in 1996 when they broke the Netscape encryption that was then supposed to safeguard Internet credit card transactions.

GSM service providers were quick to point out that nobody has managed to clone one of their mobile phones over the air, as has been done for years with analogue types. "You might as well just steal it."

Ross Anderson of Cambridge University's Computer Lab explained how an over-the-air attack might work, "When a GSM phone is turned on, its identity number (the IMSI) is relayed to the authentication centre of the company that issued it which sends back to the base station a set of five "triples".

"To break GSM, we transmit the target IMSI from a handset and intercept the five triples as they come back on the microwave link to the base station.

"The necessary microwave test set costs about $20,000 to buy but can be home built. With this apparatus you can charge calls to virtually any GSM phone whose IMSI you know.

In 1993, various governments including Britain's complained that GSM encryption was too strong for their wiretapping programmes. As EC telecommunications committee ordered weakening of the code at the spymasters' behest.

However, according to a senior British industry insider, who asked to remain anonymous: "99% of GSM calls, including internal British calls, are just handed over to government agencies..."

Pagers

In the old days, only people like Dr. Kildare ever wore a pager (aside from gangsters, that is). Nowadays, in the US more than 70% of the population carry a pager, and Britain is not far behind.

Voice pagers work by allowing you to leave a vocal message for the recipient while the more common digital pagers merely display the number.

Pagers operate in the clear on radio frequencies that can be received with any standard receiver or scanner and have, literally, provided hours of listening pleasure for scanning enthusiasts over the years.

Interception can be of considerable value in the 'spy' game. It doesn't take much time or effort to pinpoint movements, dates, times, activities and phone numbers of suspects. Then, when they have the phone number, it is easy to get the address.

There are a couple of popular intercepting pager messages. One of the sneakiest is through the use of a clone. A cloned pager is simply a pager which operates on the same frequency and has the same cap code (written on the bottom of the pager or on the belt clip) as the target's pager. In short, the paging system has no

way of knowing how many receivers are actually listening at any given time, to any message that is transmitted will be received simultaneously by all identical pagers.

A second paging intercept option is to purchase one of the fairly common software packages that work in conjunction with a scanner or a receiver and an IBM or a Mac PC. These software packages 'listen' to the scanner, which is set up to listen to a certain paging frequency. In this type of operation, the potential interceptor only needs to know the cap code of the call number.

In the case of the latter, he simply has to turn on the receiver, initialise the software and then dial the pager sending a unique code and watch the computer monitor to see when the code is broadcast. The programme will immediately display the cap code of the pager and, if it is an alphanumeric pager, the text message. After this the programme will set up an automatic file in the computer to grab any and all further messages to that pager, storing them as to time, date and phone number of text message to be called.

Fax Machines

Many people (who should know better) imagine that fax machines are a safer method of data exchange than the telephone because no words (as in speech) are transmitted: Wrong again!

This impressive invention would certainly have Alexander Graham Bell turning in his grave. First, let's take a brief look at how it works: Faxes trade set-up information at the beginning of each call in something known as the handshake period. During this time, the sending fax will set itself to the highest possible group protocol that the receiving fax will accept before it begins transmitting data. The second fax requires acceptance and confirmation of this 'handshake' before it will begin actual transmission. Some faxes provide limited security by reading the phone number of the receiving fax and comparing it to an internal list before sending the data.

What happens when you press that 'send' button is that the answering fax machine transmits a 2,100Hz tone for three seconds, and then starts a negotiating process at 300bps, including a single high-pitched tone, followed by the distinctive lower, warbling tone. When this ends, there is a brief pause and, if the calling fax hasn't responded, the process is then repeated.

The so-called 'data stream' can be intercepted by using a good dropout recorder or high impedance capacitor circuit as described above. The entire transmission may be recorded on a digital audio tape recorder. DAT's are now commercially available for about £600 but this will drop in the near future (and may already have done so by the time you read this).

DAT's use a high sample rate to record the audio in the form of Boolean digits. There is absolutely no distortion, noise or error introduced in playback or recording. What you hear is what you get – literally. Therefore, DAT's are the ideal and perhaps, really, the sole effective method of recording fax transmissions.

After the transmission is on tape, it may be either fed into a fax modem and then directly into a computer or fed into a fax machine. In either case, the information should come down a phone line.

If the interceptor has access to two phone lines, all he needs to do is unscrew the mouthpiece and clip a jumper cable from the output of the DAT directly onto the telephone line dial up the other phone line and run it into the fax machine or computer. Not difficult at all.

CHAPTER THREE

CRACKING THE COMPUTER...

Just suppose it was possible for someone to read the data being entered or displayed on your computer without that person having direct physical access and from a distance of at least seven hundred feet?

Guess what – it's already been done.

Apparently the US military has know exactly how to engage in passive data eavesdropping for some years now, but only recently were details on this amazing concept released to other interested parties.

The scientific breakthrough originated from a group of Swedish scientists who began a research project in January, 1983, to see if computers were vulnerable to information theft via electronic eavesdropping. In 1985, at the Securicom Conference in Cannes, they presented some startling proof of the vulnerability of all computers to passive information gathering.

What was actually proved here was that it was relatively easy to reconstruct data hidden in the radiated fields produced by computers, and that this did not require access to sophisticated decoding equipment. In fact, they even made the case that eavesdropping on a video display unit can be accomplished with a normal television broadcast receiver with some "minor alterations" to the unit.

What is interesting is that radiated harmonics of the video signal from a computer show a remarkable resemblance to broadcast TV signals and it is therefore possible to reconstruct the picture displayed on the video display unit by means of an altered television receiver. However, remember that this unit is entirely passive in nature and doesn't allow one to go inside the computer's memory banks or explore the RAM. Nor does it allow the operator to elicit queries. It simply receives the signal that is being 'painted' onto the video display unit of any computer (provided it is switched on at the time, of course).

It is an interesting electronic method of 'data eavesdropping' because it is completely passive and there is no bug or hidden camera necessary. The operative simply sits down at the console and reads and/or captures the data that is being displayed on the target computer!

E-mail is another area which is not nearly as safe as we may imagine which is particularly worrying these days when snail mail is becoming a thing of the past and it is easy to predict that with a relatively short period of time, e-mail will be the norm.

The Royal Mail recently issued a report which stated that their future plans included an e-mail equivalent of Special Delivery because, "users of the Internet do not have a guarantee of privacy and confidentiality, source of origin or proof or receipt. According to Jim Pang, Director of the Royal Mail's Electronic Services. "At the moment it is relatively easy either to read someone else's e-mail, or to pretend to be someone else sending e-mail." The new service will use "advanced cryptographic technology" to ensure confidentiality and authenticity. However, in accordance with the Government's recently announced proposals to regulate the use of cryptography, security services *will be able to intercept and decode documents.*

Password Protection (says who?)

The important fact to remember here is that, incredible as it might sound, passwords are not that difficult to crack. Perhaps you thought you had chosen a truly original word? Think again…

As you are no doubt aware of, most computer programmes of any importance are protected by a password which is designed to prevent outsiders from accessing or changing data stored in any of it's memory facilities. Theoretically, a password should be the ultimate protection as, depending on the type and number of characters used, it can be near impossible to crack. Note the word 'can' here because reality is that most passwords are really not that difficult to dig out because there are a number of things that many have in common.

The main one is that people tend to select a password that means something special to them (so they remember it!). And this is the basis on which many passwords are hacked.

For example, in the US recently a study was carried out where it was discovered that most passwords fall into two distinct types. One being the first name of the operator, his wife, children or pet (generally in that order – but not always!). However, in a large corporation, the installer will often use the chief executive's name as a password when he is setting up the system.

And then there are hobbies, nicknames, phone numbers and address … And the most popular password of all? You guessed it - **PASSWORD!** Which does not say a lot for the creativity of the great British public. These are the same kind of people who customise their car registration with the initials of their name.

A high percentage attack is simply to tap the computer's phone line and record in/out data. Playing this back through passwords involved in the transaction.

So, what can *you* do to protect your password? Here are some tips:

- Never use passwords with less than 4 characters. The more characters the
- better. Use randomly generated, non-word units, even if it is less convenient.
- Use a maximum of characters in the actual password. If the system permits the
- use of two words, by all means take advantage of this feature, if not, insert nonprinting or symbolic characters, such as a backspace or & in password makeup.
- Limit the number of password entry tries.
- Require a time interval between attempts.
- Provide a system for alerting security personnel if cracking attacks occur.
- For maximum security, insist on an ancillary keying method such as a physical key, card, fingerprint reader, etc.

If possible, use an authentication method that requires the host computer to match up phone numbers. In such a system, the user dials the computer, enters a touch tone code and hangs up. If the code is legit, the computer will then dial the user back and then connect him, This system does limit field access, but provides excellent security and several commercial systems are available.

Database Access

What is a database? Simply a collection of information available on line and, in some cases, in hard copy text formats. Databases can exist in any computer and some large databases are present in a number of computers on a net, simultaneously. Information is usually fed into a database by hired readers who scan sources of information including most major newspapers, journals, graduate theses, books, newsletters, technical and scientific papers, popular magazines, court cases, etc., just about everything is available on one database or another....

This information is read by the input person and then typed into the database. It is also cross-indexed by title and keyword which is an important concept when it

comes to access. There are literally thousands of commercial databases which are online and can be accessed by anyone with the correct gateway, a computer, a modem and some knowledge of how databases work in general, together with a few techniques for the database or the database provider that will be utilised.

Just to illustrate how accessible commercial databases are today, it is a fact that any decent newspaper now runs a database search as a prerequisite to writing an important story. This search may turn up important information that can be used to research the story or may even turn up the bare bones of the story itself by simply expending a few minutes of the investigator/researcher's time.

But investigations via the database can go further than this. For example, a specific search on a person's name will often bring up background information and lead to his or her whereabouts. I personally know of a case where someone needed to find some information on a fairly well respected businessman. He suspected the man would belong to a prominent club, a rather prestigious organisation for businessmen (which I dare not mention as I'm likely to be sued), and thought that he could probably get information from some of the man's cohorts and competitors. He called the Club only to be rather less than politely rebuffed about the possible availability of any membership roster on their part. Such things were simply not done.

Under normal circumstances, he might have gone to a number of meetings, staked out the car park, ran license tag searches and gradually tried to sift his way through a mountain of information. Instead, he merely punched up a database, punched up a listing of *Who've Who* (on line and available) and then did a key word search using the name of the Club as a delimiter. As might be expected, persons who write their entries in Who's Who wish to impress their professional organisations; for instance, the Club, to which they belong.

In a matter of seconds, he had a list of almost the entire membership of the chapter of Club that he was looking for, plus contact addresses, background information and methods of social engineering access on every member at his fingertips.

It took two phone calls to find out exactly where the subject was, what the man was doing and what he had done to both the contacted members of the club - and (in this case) the client of my acquaintance....

CHAPTER FOUR

VIDEO SURVEIILLANCE

Video surveillance is essentially the ability of putting the operator's eye into remote area and recording the signal. It is no more complicated than audio surveillance, all that is required is to connect the correct cables to the correct equipment. The key is the creativity involved.

Video surveillance is nothing new. More than fifteen years ago, electronic hobbyist magazines were advertising video cameras that were no more than a couple of inches in size, battery run and which could, naturally, be easily concealed in anywhere from a stuffed animal to a pot plant!

The newer charged coupled device (CCD) video cameras can operate well under low light conditions and have another advantage over the standard tube type consumer-grade video cameras - they can be made much smaller and can also see infrared light sources.

What to look for? Well, an infrared TV remote looks like a little penlight through a CCD video camera. A surveillance operative who needs to get choice video under very low light conditions will use a CCD video camera and an infrared light source. The latter could be as simple as a spotlight with an infrared filter covering the spotlight lens. An unsuspecting person can be fully illuminated and not have a clue that every move he makes is being observed with ease using CCD video or night vision devices, as you can't see infrared light with the naked eye. There are two general terms for describing night vision devices:

1. Active - This type requires an infrared light source in order to be of any use and was the first night vision device available on the market.
2. Passive - Commonly referred to as "starlight" because it only requires starlight or moonlight to operate. This will actually amplify starlight and moonlight via a large magnification factor. It's also been around for a long time and is the most popular of the two. Starlight scopes have adapters that allow their use with tube-type video cameras. Starlight scopes can also be enhanced for very low light situations by adding an infrared light source.

There are several well-known companies that install pinhole lens video cameras and have had many years' experience installing video systems in retail stores,

offices and government building. This is big business and far more widespread than security personnel care to admit. Covert video cameras can be concealed for extended periods of time. For example, installed in a ceiling in such a way that you could stand directly below and stare at the ceiling for hours on end and would still be unable to spot the tiny concealed lens.

How do they work? Video cameras traditionally use a tube to convert light into an electrical signal. These tubes can be a mere half-inch in diameter, although the larger sizes generally provide a superior picture. However, more recently, solid state chips have been replacing tubes in cameras. These chips have approximately 360,000 "holes" or pixels that each capture a small piece of the scene and then dump it out to the camera circuitry many times a second.

Chips have several advantages: firstly, they don not "burn in", secondly, they last several years and third, they start up instantly and will not break if the camera if subjected to rough treatment. They also do not smear as much as their tube cousins do and are small enough to allow sub-miniature camera sizing. Cameras do exist that consist of simply one chip with a lens built into the surface, but the price break (at least at the time of writing) is fairly substantial between the two size category and there's really few placements that would justify the extra expense.

Most of the cameras used in surveillance applications are black and white only because there is really no need for the extra expense and bulk of a colour unit. They are almost always brought in from a couple of Japanese manufacturer - the little circuit board mounted unit sold by almost everyone is in reality a Chinnon, made in Japan. It should also be noted that because this camera is actually mounted directly on a foldable circuit board, it is the unit most often used in expensive re-proportioned camera units like PC's body pack where the boards are unfolded and worn in a hidden belt or vest.

Camcorders are starting to appear in surveillance work, especially the smaller 8 mm based units. Consumer camcorders are really not applicable to this type of work because they do not have interchangeable lenses as do the professional C-mounted camcorders. If one attempts to mount a pinhole or other specialised lens on a fixed lens camcorder the light gathering ability drops off rapidly.

The pinhole lens provides a unique opportunity for covert viewing, photography or videography. The actual lens is tiny, one tenth of an inch in diameter which can be attached to the front of any camera, or in some cases, are constructed as an integral part of the camera itself

Pinholes are designed to reproduce an entire scene through a small hole in some solid barrier. If the unit is to be mounted within the target area, applications could include radios, file cabinets, mounted above dropped ceilings or stashed inside most common appliances. They are constructed with varying angles and degrees of fields of view. A number of charts, including one will show exactly how much of a certain room size will be covered with any lens. This allows someone to pre plan the installation by drawing the target room, on a piece of paper and detailing the area to be observed.

The lens is sometimes positioned behind a shared wall with only a minute hole opened into the actual target room. In this case, the lens must be positioned tightly against the wall so its entire field of view is passed on to the camera. Pinhole lenses are configured in a variety of styles, lengths, and speeds. The perfect lens would be tiny, fast and process a large field of view. In reality these factors are in a constant tug of war as the light gathering power of any lens increases times four with a doubling of the lens size.

Nowadays, very speedy lens has become available on the general market which provide a good field of view and a high lens efficiency. These lenses are available in straight or right angle configurations.

Most are fixed focus in design, allowing a reasonable depth of field and a high recognition factor. Some pinholes are now produced with automatic iris control for a variety of lighting conditions.

Most speciality lenses are set up to accept a third inch Vidicon camera which works best with moderate to high light level provided by sunlight or fluorescent sources. If the application is one with a lower light level, then a more sensitive Newvicon, silicon or chip camera can be used which will react to lower levels of light as well as to IR light which allows invisible "boosters" to be secreted in the target area.

These latter cameras do require some sort of auto iris to control the amount of light that reaches the tube/chip either in the camera (electronic or optical) or in the lens

itself. A good electronic iris will have a range of 300,000-1 in order to compensate for low light conditions or day-to-night changes.

Night Vision

There's no question about it, we humans have a problem to see in the dark; limitations imposed by our biology. In short, we are only able to see things at a certain light level. To do otherwise requires a system of electronic enhancement.

The person responsible for the idea behind night vision devices was coincidentally the very same person who gave us the idea of curved space and atomic bombs (among other inventions) - Alfred Einstein. He discovered that if he took a piece of matter and hit it with a ray of light, it could be induced to give off electrons.

Atoms consist of both positive and negative particles and when a ray of light strikes some atoms, they take on the extra energy provided by the light and free up an electron. After this theory was discovered, someone else decided it might just be possible to actually start a flow of electricity using light energy.

The people who came up with the very first infrared devices tested materials until they got an element with this property. Next they were able to find a wavelength of light that was particularly useful in this application and they were able to cause electrons to jump from one spot from a negatively charged electrode to a positively charged electrode. At the positive electrode a phosphorescent screen was added and the first infrared device was born.

And it's easy enough, all that is necessary is to hook a battery up and charge the screen to a positive value and the electron gains energy when it bounces off. When it runs into a phosphorescent screen it actually gives off light. In this process, light energy being transferred to electrical energy and then as it hits the phosphorescent screen it back to light.

Interestingly, the first practical uses of this old infrared technology dates back to the time of about the second World War, it is now known as zero generation night vision.

Some of these early goggles are still available today. They are usually advertised as Israeli surplus night vision goggles, and sell for about £250. The sole way these are able to function in today's environment, however, is if the operator provides a very bright IR light source.

Next, the engineers came up with a better device by changing the metallic substance. Some substances, when placed on a photo cathode changed all light, include the visible variety, into moving electrons.

They were then able to activate a phosphorescent screen and see the other image on the other side.

Two major areas of concern remained: Most light, even in daylight, was too weak to kick loose enough electrons to me the unit function, a system for amplifying the available light was required.

The other problem was that as the electrons bounced around they acted incoherently, scattering their energy unless the plates were placed almost on top of each other or the electrical potential was dramatically increased.

To close this chapter, I would like to include the following report which I feel aptly demonstrates just how widespread camera surveillance work is - and how it can be affecting every one of us - *right now!*

King's Lynn, on the Great Ouse in Norfolk, is a town of some 30,000 inhabitants within a borough catchment area of a further 100,000 people. An important port from mediaeval times until the last century, its many historical buildings contribute to its present position as a centre for East Anglican tourism.

In 1992, King's Lynn made headlines as the first town in Great Britain to introduce a comprehensive closed circuit television scheme designed to combat local crime. Seventy cameras kept watch on car parks, housing and industrial estates, leisure facilities and around the town centre. They feed pictures, on a round the clock basis, to split screen televisions in the central council run control room. As it arrives, the information is monitored by trained staff and simultaneously taped on video recorders. Any crime or suspicious incident caught in progress is relayed to screens in the nearby police station.

Support for the scheme, apparently, is high. Consultations with the local population, before and since the scheme's introduction, seem to have allayed any fears that so much intrusive security might threaten civil rights. Women on there own, and elderly people, now have the confidence to pass through areas previously considered dangerous.

(Now comes the interesting bit...) The Council admits to the possibility that such a system could be abused by politicians and the police and is in the process (after how many years?) of up dating its original Code of Practice, stating precisely who is permitted access to the control room and the tapes and the conditions governing the use of the cameras. For example if, during a camera's sweep along a street, it is able to see into someone's sitting room or bedroom, at that point it will be programmed to switch off for the time it takes to pass that point, or a fixed metal flag on a bracket in front of the camera will obstruct that part of the lens' view.

"Everyone is happy with the system," says John Huston, speaking for the Council. "We insist on being completely open in our approach to combating crime and we have had no complaints whatsoever. Since we began the scheme, we have had visits from 350 representatives of other towns and cities, even from abroad, and most have left to start up their own systems. How many other places have followed our lead? It's easier to ask how many have not. CCTV surveillance is becoming the norm in Britain, and why not? We all have civil rights, including the right not to be victimised by criminals.

"The reasons for the success of this technology are clear. The deterrent value of the camera has dramatically reduced the crime-rate. Theft of and from cars in King's Lynn has dropped from 190 per year, before CCTV, to 4. Vandalism has been cut by 91%. And we can count 800 arrests since 1992, directly attributable to CCTV.

"We have apprehended two absconders on bail, helped solve 70 burglary and 80 criminal damage cases, caught four credit-card crooks, brought to book 71 driving offences such as entrance-blocking an double-parking and assisted in cases of arson and assault. The crime we don't deter, we detect."

Which is all very well for the middle class burglars of small town Kings Lynn, but what if...? What if a Hitler or a Stalin slipped through the democratic system and gained autocratic power in Britain? Of course he would brush aside Codes of Practice and make use of any existing CCTV, especially in large cities like London, Manchester, Birmingham and Glasgow.

Although, if these systems were not already in existence, it would take an efficient dictator just six months, at most, to create them.

CHAPTER FIVE

THE 'CLASSIC' BUG

There are countless ways to bug a conversation, which is pretty worrying when you are on the receiving end. Plus, even someone with severely limited funds and technical know-how can successfully bug a room.

For a start, remember the baby monitor that perhaps you once had? That neat little contraption that would pick up those cries, even if you were the other end of the house? Think about it. In exactly the same way, an amateur bugger could pop into Mothercare and pick one up, then hide it in his home, office, flat or other room of interest behind a rarely moved appliance, picture or item of furniture. He can then be up to several houses away and still listen in on all the conversations in the room of interest with the companion receiver, which is sold along with the baby monitor. The monitor is quite sensitive and are normally crystal controlled which prevents frequency drift. If necessary, wireless baby monitor reception can be easily enhanced by using a police scanner with an outside antenna instead of the supplied receiver.

Another inexpensive bugging option is an intercom system, either the wired or wireless variety. For example, say a director of a company was concerned about the loyalty of his employees, he could simply place the master unit in his office and the so-called 'slave' unit where his employees worked. Then, all he needs to do is switch on and he can listen to every word of their conversation. This is a far more common tactic than most of us imagine!

And then there are the wireless studio or lapel microphones which are readily available at major electrical and audiovisual shops. The more inexpensive models are limited to around a 300 foot range, while the top of the line variety can extend to an impressive quarter of a mile range (under the right conditions). The latter are referred to as "diversity microphone systems", use two antennas and don't 'drift' as the cheaper models tend to do.

The wireless microphones resemble tiny broadcast stations and should be worn on the body. The capacity is excellent. I have personally witnessed that, even the cheaper models, will pick up a whisper in a room from 15 feet away (or more) and broadcast it up to 200 feet away! Most of these studio or body microphones come

with a companion receiver. Some unpleasant people have been known to hide these microphones in rooms.

These three devices listed above are very inexpensive. Wireless baby monitors are available for £40 or less, wireless intercoms for £60 or less, and hard wired intercoms for as little as £10. Worrying, isn't it?

To further demonstrate just how easy 'bugging' can be, picture the following. The amateur spy can either buy a bug through underground sources or purchase a ready to assemble kit from various suppliers which advertise in electronics magazines. At the time of writing (ironic as it may sound!), it is illegal to possess or transport a device that is specifically for eavesdropping, although it is perfectly okay to sell or buy a bug or 'tap' in kit form. Naturally, baby monitors, intercoms and body transmitters are exempt from the law, as long as they are 'supposedly' used in the manner for which intended.

As mentioned, a bug can be placed virtually anywhere in a room (but preferably away from large metal objects, as this can disrupt the transmitter and clarity). Two or more batteries can also be connected in parallel in order to provide increased transmission time. For example, four days, instead of two. Once the bugging transmitter is placed, all that is required is to set up a listening post which could be a car, rented office, garage, or flat. A tabletop portable FM radio, a signal activated switch and a tape recorder are all that are required for the perfect bugging operation. That easy!

An alternative to this technique is a correctly placed voice operated transmitter, plus radio with a VOX tape recorder. The advantage of this particular system is that the bug does not transmit unless someone is talking or making a noise. Detection of a VOX operated bug is somewhat reduced since it is only on when someone is actually speaking.

Think about it ... there is a very obvious way that these automatic recording systems can be sabotaged. That's it! All you have to do is turn on a radio, stereo or TV to a reasonable volume and then leave it on all day and night. The bug will pick all this up very clearly - tape after tape after tape and, chances are, that any conversation will be completely drowned out. Simple yet effective.

Another time-honoured amateur bugging technique is to use carrier current transmitters that utilise extremely low frequencies (below the AM broadcast band), these use a building's wiring for their power and signal path and rarely transmit much beyond the building where installed. Thus, the 'bugger' need only rent an office or apartment in the target's building and then hide a carrier current transmitter in their room. The transmitter will last indefinitely, and most so-called counter-measures personnel probably will not detect it as the majority of readily available counter measures gear is not designed to detect such low frequencies.

On the whole, the generic hidden transmitter locators sold in the LJK don't work too effectively in urban and suburban areas due to the high levels of radio frequency energy floating around. However, a good countermeasures team will always use a spectrum analyser which looks very like an oscilloscope.

Yet another technique that might be used by an amateur is a unique bugging device which has been around for close to forty years. It has a variety of names, including 'harmonica bug', 'infinity transmitter' and 'coast-to-coast transmitter'. Before the phone company switched over to the electronic switching service, this transmitter could be simply connected to a phone line and hidden in a room on the target's premises. The person bugging could then call from essentially anywhere he chose in the world, send a certain tone with a portable tone generator over the phone line and the device would answer and permit the listener to hear all the conversations in the room - and without disturbing the normal operation of the phone or alerting the target. The 'infinity transmitter' would answer before the first ring but when the target picked up the phone, everything would return to normal.

Naturally, when the telephone company upgraded the phone system to the newer ESS system, these transmitters became defunct, however some companies have redesigned infinity transmitters to enable them to work with the new systems. But there are tell tale signs to look for if you suspect that you are victim to such a 'bug'.

Firstly, there will be one ring and then, less than two minutes later, another ring. If the target picks up the phone after the first ring, it will disrupt the operation of the device, causing the operative to initiate another activation cycle. In other words, he will have to start all over again! Also if he (or she) uses an outdated infinity transmitter with the new phone lines, the phone will ring just once and then anybody

who tries to call while the transmitter is activated will just get a busy signal. A second problem which can occur is that the phone rings just once and the infinity transmitter will answer. The caller will then be treated to five to ten seconds of room sounds or conversation before the 'time-out' (hang-up sequence). However, the new generation of 'smart' infinity transmitters will automatically disconnect when someone calls, thereby allowing the phone to ring.

Professional bugging is a far more sophisticated operation. For example, the pro can quite easily construct a circuit that will make any battery-operated transmitter AC operated. He may also buy circuits that allow him to shut off the bug remotely if he hears a person conducting a countermeasures sweep.

The pro may also use complex modulation methods for his transmitters that might not be demodulated or detected by most countermeasures, such as via using a very low-power transmitter that can slip past detection.

A pro may also simply use a microphone which is wired directly to the listening post where the tape recorder is sitting. There are microphones available today that you would literally need tweezers to handle they are so tiny and which can be connected with either very fine wire or conductive paint. A clever pro might install a tiny microphone, run a long length of fine wire to it and then hook up the wires at the other end to a hidden transmitter. The truth is that microphones cannot be detected without a pretty thorough physical search as they don't radiate any detectable fields.

Finally, let's not forget vehicle bugging. There are some very effective bugs made just for bugging vehicles which are generally placed in line with the vehicle's radio antenna. These units are typically sold to law enforcement, complete with an automated receiving system.

But also available is the 'bumper beeper' which, in a nutshell, is an electronic 'Package' that can assist someone to successfully follow a vehicle under surveillance. A quality unit, specifically designed for covertly tracking a moving vehicle and operated by someone who knows what he is doing, will let the operator hang a considerable distance behind the target vehicle and indicate what direction to travel in order to stay behind him.

Bumper beeper packages consist of a transmitter which is usually affixed magnetically to the car under surveillance and a companion receiver which will tell

you certain things about the conditions between the transmitter and the receiver. Cheap units can be found for around £300 which will tell you only if you are moving closer or further away from the target. Slightly superior units will indicate, either by a zero centre meter or a series of lights, where the target vehicle is located in reference to your vehicle. All units which indicate a bearing also will give you a relative range. Properly applied and used, a real beeper ('real' meaning not a toy) will let you stay far enough behind the target to be well beyond visual range. By glancing at the receiver's meter panel every so often as you drive, one can soon learn quite a bit about where the target exactly is.

If for whatever reason, you decide to buy a unit, plan on spending several hours reading, not only the technical manual for the unit, but some information on radio direction finding in general. Knowing just a bit of the theory of direction finding (which is what the bumper beepers really do) will help you get much more out of the unit.

A decent beeper receiver designed for investigative use will track accurately on signals that are inaudible through the speaker, so if things get difficult, keep the sensitivity at the absolute minimum necessary to get a definite indication on he meter, As long as the meter is reading, don't worry that you can't hear the beep through the speaker.

Some tracking systems provide 180 degree performance and some even offer 360 degree. What this means is that the 360 units will track on targets both in front of you and behind you, although the 180 degree systems will only indicate correctly on targets in front of your vehicle.

CHAPTER SIX

COUNTERMEASURES, TIPS AND TRICKS

The most crucial part of any countermeasure tactic is a detailed physical search. True, that fancy electronic equipment is terrific, but what if the bug isn't in use any more? What if the battery's run down? What if the bug is equipped with a switch so that, if you are detected, it can be simply turned off?

When planning a countermeasures survey, it is similarly important to determine whether or not it is a problem if the people who are listening are aware that there is a search in progress. Most of the time, of course, it is.

Take an office search, for example. Start with everything available, from the top and then work down. Particular attention should be paid to anything that has a battery in it or that plugs into the wall, as well as things that may have been gifts.

What is the best way to plant a bug without committing a burglary? Give it to the target, of course. Take a calculator, for instance. It's not difficult to conceal a transmitter here. Likewise, the telephone has its own power and is often used as a bugging device. Turn over objects on the desk and look for transmitters. The typewriter is plugged into the wall and an ideal hidey hole. There may be computers, a local area network. Who uses these items? The target and his secretary...

Yes, a physical search means examining every single thing. Looking in books, under books, behind books, behind pictures, curtains (popular place for a bug), lamps, plants, calendars, every place and any place. Take the time and, in particular, take note of anything that seems out of place. I even know of one ingenious 'bugger' who placed a bug in an envelope, sent it express delivery with the words *'Private and Confidential' printed* on the front, well aware that the person concerned was away on holiday for a couple of weeks so it would sit in a prime location on the desk in the meantime. This is possible because these days, bugging units can be so flat.

However, don't forget that most bugs, especially those which work on a battery, have a limited life span. How long? Well, it depends on the bug, the power output and the batteries involved. In general, it's safe to say that a bug will last anywhere from one to three days. This means that most people will not just go in, take a risk, plant a bug on a random basis. Most are targeted for a specific period of time.

Is there an important conference coming up? A budget meeting? Are the design engineers getting together? These are the sorts of occasions to be wary of - and right beforehand.

Another common practice is for the unit to be hooked into the mains where the power lines come into the office. There's no limited life span here and the easiest, most practical way to bug in this instance is via hiding a tiny microphone in the room and attaching external wires. Again, hard to find, and a good reason to take a very good look at any suspect looking wiring.

A physical search for bugs should include all telephones in the area. The first thing to do is disassemble the phone and look for things that shouldn't be there. This is known as the strip, search or the sneak and peek. Take a good look at that microphone button and ensure nothing is clipped on the wires or stuffed up inside the handset.

And, while on the subject of phones, remember that telephone tapping is the most common mode of electronic eavesdropping. Automatic telephone analysers are available from a number of companies, most based on the mid sixties Mason Engineering design. They are fairly efficient in detecting taps as they are designed to find audio on the phone lines by cross-checking all the possible combinations. In itself this is a good test, although it can be performed with a stand-alone amplifier and some patience.

One method that has been used to trap eavesdroppers is to have a voice activated recorder on the line that is suspect. There is a good chance that anyone tapping the line will call in after hours to test out his unit.

The simplest, easiest and cheapest step in bug hunting is to take an all band radio, turn the volume up high and tune through the bands. In order to use the all band radio as a device to locate bugs, turn the volume up and place it in the room where a suspect bug might be (if the possibility of alerting the people who might be listening poses no hazard). Now, tune through all the frequencies. When the radio is tuned across an active frequency, feedback will immediately occur. Back off slightly and local audio will come through.

The reason this works on many small transmitters is that bugs don't have coils to suppress harmonics (signals that are doubles and triples of the original frequency).

Countermeasure Tricks and Tips

Here is a short list of well-tested tricks to play on those persistent eavesdroppers in your life:

- Turn radios, TV's and stereos on at a reasonably high volume. Most bugging devices will be overwhelmed and the audio quality turned to mud with loud music or noise.
- Stand or sit close to the person you are conversing with and keep your voices down.
- Take the phone off the hook on a random basis and place the handset close to a stereo speaker playing some particularly obnoxious music.
- Avoid using cordless phones
- Use a voice disguising telephone if possible. It will make your voice totally unrecognisable.
- If you are having a meeting or discussing sensitive subjects in either an office or home, unplug the telephone from the wall jack.

Fact or Fallacy

Question: "I have been told that a good countermeasures team can tell whether my telephone is tapped at the telephone company's central switchboard."

Answer: "False. Electronically, there is no way to tell if there is a tap at the central switchboard. The electrical characteristics of the phone line may vary from one central switchboard to another.

Question: "Some people have said that they can hear most telephone taps clearly on their line."

Answer: "Not true, unless some wire tapper is a complete moron and using defective equipment, that is."

Question: "Is there a number I can dial that will tell me immediately and with certainty whether my phone is being tapped or not?"

Answer: "Nice idea but afraid not!"

Question: "I understand that a countermeasures team should be able to debug my home or office in two hours or less."

Answer: "False. Unless you live in a one room studio, a half a day to one full day is far more likely."

Question: "Any countermeasures team chosen at random from the Yellow Pages will be able t o find a telephone tap on my phone line, assuming that it has been tapped."

Answer: "False. There are at least three methods of telephone tapping that will not be detected by the best, most sophisticated intelligence agencies in the world. (Sorry!)

CHAPTER SEVEN

SELECTING THAT COUNTERMEASURES PERSON WHO IS RIGHT FOR YOU!

If you have decided that you definitely need the help of a professional countermeasures person then there are certain qualities (including qualifications and experience) you should look for, including the following:

1. Does he know the basics of the frequency spectrum, basic frequency allocations and basic propagation characteristics of commonly used frequencies?
2. Does he own a police scanner and use it on a regular basis? Is short wave listening and scanning an ongoing hobby?
3. Does he know the approximate bandwidth of his radio detection equipment?
4. What kind of equipment does he use to find hidden transmitters?
5. If he doesn't use a spectrum analyser, does he use a near field receiver and various radios that cover a wide portion of the frequency spectrum?
6. Will he let you watch? If not, definitely go somewhere else.
7. Did he tell you that there are certain bugs that cannot be found unless you literally tear the place apart?
8. Has he done any electronic experimentation and design work?

If he answers "no" to any of questions, 1,2,3,5 or 6, look for someone else. if your primary concern is phone tapping then ask the following.

1. Has he ever done any office or residential phone installation?
2. Does he understand the basic electrical characteristics of phone lines, including voltage, current, impedance and so on?
3. Is he aware of the fact that certain taps cannot be detected?

If his answer is "no" to any of these questions, look for someone else.

CHAPTER EIGHT

LEGALITIESS & PRIVACY LAWS

There is actually not a lot to say here because, there are regretfully very few lawyers who are knowledgeable about communications privacy laws. I have personally met a number of eminent professionals in the legal field who are not even aware of the fact that bugging and tapping are illegal. In fact, it is estimated that, for every legal, court ordered electronic surveillance conducted by law enforcement agencies, there are at least one hundred illegal surveillance operations being carried out.

As for privacy laws, as we all know, the tragic, senseless death of Diana, Princess of Wales, whether due to driver-drunkenness or not, has dramatically highlighted this issue.

Consider, in past years, the saucy vicars, and others, exposed in *the People* and the *News of the World* by envious hypocritical parishioners. Consider those thousands of lives destroyed, when their only mistake, often, was to be human.

Consider, more recently, the actors, sports people and politicians who failed to realise that they were not allowed to behave like their ordinary neighbours.

Consider us, the insatiable audience greedy for juicy stories we can tut over and our envy of the rich stars we can never be.

We are aware of, and become angry at, bureaucratic incursions into our political and financial right to privacy. However, most of us have never been unlucky, famous or downright naughty enough to gain anyone's attention (on a wholesale public level, that is). We have always accepted and chuckled over, the long-standing Sunday papers tradition out of which has grown the current lack of celebrity privacy. Now, however, the nature of the attack has changed to something more vicious and predatory.

Notwithstanding other factors, there can be no doubt that Diana's death was caused by those members of the press known as the cr6me de la scum. Dodi Fayed's (possibly) drunk driver would not have reacted and died, if the paparazzi had not been in motorcycle pursuit of the Princess. The death of three people in a car crash in Paris was undoubtedly caused by the dangerous attention of photojournalists whose

looseknit international group, over many years, had already reduced Diana's life to a telephoto cartoon strip.

It is true that Diana tried to manipulate the press, sometimes for the sake of her charities, often in her own defence, but her touch was faulty. She failed to put over her side of the unequal fight with the Royal Family and sometimes made mistakes with her charity image. It needed her death to bring nostalgia and wisdom, albeit after the event. She also failed in her oft-repeated request to be left alone by the press. Her right to privacy should have been respected and it should have concerned us that it was not. At the time of writing, at least, it is apparent that the paparazzi are being slightly more sensitive. For example, the young Princes are being, for the most part, left alone to mature in piece. The question remains ... how long will it last?

CHAPTER NINE

CONTACT LIST DIRECTORY

The following comprises a comprehensive list of surveillance equipment and suppliers in both Europe and the USA. The majority produce their own product catalogue which may be ordered via written request.

United Kingdom/Europe
ABUC, Sicherungestechnik GMBH Drehomstrasse 7, W 3000 Hannover 51, Germany
Surveillance Cameras

ATET VG Da Verrazzano, 42, 1012 Torino, Italy
Tiny crystal controlled transmitters in the 700-900 Mhz range

Audiotel International Ltd., Cavendish Courtyard, Sallow Rd., Weldon, Corby, Northants NN17 1DZ
Unusual diversity of counter-surveillance and surveillance equipment,

C. Systems, PO Box 108, Leeds, LS14 6YR, Tel. 01976 620 194
Provides total service and product line, including bugging, transmitters, vehicle tracking system, counter surveillance, covert, IW, VHF, infra-red cameras, voice stress analysers, telephone taps, room bugs, infinity devices, telecorders, transmitters crystal controlled, microwave transmitters, bug detectors, etc.

C.A.Z. London, 39 Star, St., London W2 1QB
A unique organisation who manufacture their own products which they export to about 50 countries, including night vision, x-ray systems, recording briefcases, Scanlock receivers, dialled number pen registers, cigarette lighters, sub-miniature transmitters, parallel phone taps, car bomb protection systems and a number of other items so secret that they are not even included in the catalogue!

Communications Devices Ltd., 6 Riverside Park, Dogflud Way, Farnham, Surrey GU 9 7UG
High level facsimile monitoring systems, loop extenders that read pulse voltages as well as on and off hook currents and then regenerate same to hide activated tape recorders and complete telephone monitoring systems that will monitor from 10 to several hundred lines in one fell swoop.

Complete Security, 14 Hollywood Rd., London SW10 9HT
Anti-terrorist equipment, surveillance and counter-surveillance equipment that cannot normally be found within the USA.

Covert Transmitter System, SDMS Systems, 365 Fulham Rd. London SWIO 9TJ
OEM supplier of a modular audio surveillance system that can be adapted to a body wire, phone transmitter, car bug, mains transmitter or normal room transmitter. High power, upper FM ranges, designed for law enforcement or security. Included are adapters, receiver, slow speed recorder and "detailed instructions". Very competitively priced.

Datong Electronics Ltd., Clayton Wood Close, West Park, Leeds LS16 6QE
Upper level counter-surveillance equipment, including Scanlock type receivers, direction finders and their 'Ranger' which introduces its own sonic footprint into the room, listens for an audio return and then calculates the exact distance to the bug, helping the operator do an immediate locate.

Eckert Instrument Company
109 Pinecrest Drive, Annapolis, NM 21403
Suppliers of general surveillance gear from Europe and America.

Eleektron S.A. PO Box 39, 842 10 Pernes, France
Long time surveillance and countermeasures supplier. Offer several unusual products, including scrambled recorders and transmitters.

Grimm Sicherheitsetchnik GmBh Hittfeider Str., W 2107, Rosegarten, Germany
Building and room surveillance systems. CEM

Idesco Oy Teknologiantle 14, SF 90570 Oulu, Finland
Surveillance Equipment Manufacturer

Indigo Active Vision Systems Inc, Techopole, Bush Loan, Edinburgh, ER26 OPJ
Tel 0131 475 7200 Fax 0131 475 7201
Indigo supplies video networking technology to OEM's and specialises in digital technology. The company provides everything for video networking, from capture through compression to TCP/IP transmission, onto a single device.

Lorraine Electronics Surveillance, 716 Lea Bridge Rd. London EIO 6AW
Lorraine is one of the most comprehensive OEM suppliers of ES gear in the world. Their selections fall into a couple of different stratas moderately expensive, corporate level systems and lower priced transmitters, wall contact units, infinity transmitters, etc Their lower priced line (Ruby Electronics) seems to share many products with Micro in Japan.

Micro and Security Electronics, Efftngestr. 19, 2000 Hamburg 70, Germany
Another very slick producer of high level surveillance and counter gear, including full rack telephone monitoring gear and portable satellite communications stations to crystal controlled belt transmitters and full briefcase Keltype eavesdropping systems.

Optical and Textile Ltd., 22-26 Victoria Rd., New Barnet, Herts EN4 9PF
Suppliers of sub miniature (Toshiba) cameras.

Pedi Ag Kolikerstrasse 17, CH 6036 Cherenfeiden, Switzerland.
Personal Detection Systems

PK Electronics, Heidenkampsweg 74, 2000, Hamburg 1, Germany
(or 405 Park Avenue, New York, NY 10222)
For years, PK has been one of the, if not the, largest supplier of exotic surveillance equipment in the world. They have expanded from the original location in Germany to Paris and London. PK's equipment is just this side of amazing, from night vision gear, fax interceptors, scrambled bugs, exotic digital telephone line analysers to tiny stick on transmitters that look like a piece of a piece of plaster on a nail and belt mounted video camera/ recorder combinations. PK has got just about anything anybody could possibly want in the field of surveillance.

Puretone Ltd., 10 Henley Business Park, Trident Close, Medway City Estate, Rochester, Kent ME2 4ER
OEM supplier of inductive receivers and covert radio accessories.

SDMS Security Products, Ltd., 365 Fulham Rd., London SW10 9TJ
A distributor of really interesting security and surveillance supplies including the grapnel shooter, Kevlar vests, contraband detectors, search kits, X-ray equipment, telephone surveillance units, video surveillance gear, scramblers, shock batons and much more,

Security and Defence Marketing Services Ltd., 14 Hollywood Rd., London SW 10 9HT
Electronic counter-surveillance gear.

Security Research Limited, Cavendish Courtyard, Sallow Road, Corby, Northants NNI7 1DZ OEM
Supplier of excellent surveillance equipment from the thru-wall accelerometers, FM transmitters, carrier current transmitters, night landing systems, cameras, telephone, telex and fax monitors, microwave video links and a host of other equipment not found anywhere else.

Sipe Electronics, POB 2371, 4150 Krefeild 1, Germany
A most unusual surveillance supplier offering such units as the SIPE MT, a solar powered room transmitter hidden in the bottom of a whiskey glass. The tiny transmitter is invisible to the naked eye and the solar cells are arranged on the bottom of the glass just like an ornament. The transmitter turns itself off automatically when the glass is turned upside down. Particularly ideal for those diplomatic get togethers...!

Sonic Communications Ltd, Communications Centre, The Green, Castle Bromwich, Birmingham B36 9AJ
Upper and police and paramilitary equipment, including wireless headsets and VOX operated microphones for walkie talkies, ultra lightweight headsets and a new video/ still briefcase recorder system.

SUMA Designs, The Workshops, 95 Main Road, Basterley, Nr Atherstone, Warwickshire CV9 2LE
The SUMA kits include: The SCRX Subcarrier Room Transmitter. Room audio is coupled to an ultrasound carrier which is then transmitted to a special receiver which demodulates the carrier. Normal receivers will hear absolutely no sound on this frequency. The SCLX does the same thing for a telephone line. The SCDM Subcarrier Audio Demodulator receives audio from the earphone jack of your receiver, filters out the ultrasonic carrier and amplifies the audio while demodulating it from the carrier, as well as narrow band transmitters, remote controlled transmitters and so on.

Trend Telecommunications Ltd., Knaves Beech Estate, Loudwater, High Wycombe, Bucks. HPIO 9QZ
Encrypted fax machines that meet Tempest standards.

Wood & Douglas, Unit 12-13, Youngs Industrial Estate, Aldermaston, Reading RG7 4PQ
Security monitoring specialists who make a carrier current video transmitter and receiving system allowing one to send both video and audio over existing AC supply lines.

Far East

Cony Mfg. Co., No 27 2-Chrome, Kangetsu-Cho, Chkusa-Ku, Nagoya 464, Japan
one of the pioneers in miniature telephone taps and room transmitters.

Elestrong Corp., POB 68-291 Taipei, Taiwan, ROC
Ten years experience in the making of FM microphone pens, FM wireless transmitters and telephone eavesdropping devices.

Kant Corporation, Shiba, PO Box 145, Tokyo, Japan
Kant is one of those Japanese companies that everybody wants the address of because they produce ingenious tiny surveillance devices. In this case, primarily transmitters and receivers which are quartz controlled and operate outside conventional bands. Kant's equipment is purchased by many spy shops and surveillance re-sale agents, then market up several hundred percent so it is advisable to contact them direct. They are also one of the only places where you can find a crystal controlled series telephone tap and matching receiver, excellent little dropout recorders and a vibration detector.

Kato International, 19-18 Jinguamae, 2-Chome Shibuya-Ku, Tokyo 150, Japan
Manufactures inexpensive, yet effective surveillance equipment,

Micro-Electronics, 1 Kada Bldg., 1-3-16 Shintomi Shou-Ku, Tokyo, Japan
Manufacture and sell miniature transmitters and other surveillance equipment.

T. Satomi & Co. Eastern Cross, Akiba Room 506, 29-3 Taito I-Chome, TaitoKu, Tokyo, Japan

Supplier of about 50 different bugs, taps, trackers, receivers and a 'Handy Car Chase Radar' system.

U.S.A.
Surveillance manufacturers and suppliers are located throughout the United States and, obviously, there is not enough space to include them all here. Instead, I have tried to list those that I either know of personally or which are part of a respected chain.

Communication Control Systems, Headquarters, 360 Madison Ave., 6th Floor NYC 10017
CCS, 1435 Brickell Avenue, Miami, FL 331331
CCS, 444 Madison Avenue, NYC 10022
CCS, 1420 K St. Suite 510, Washington, DC 20005
CCS, 9557 Wilshire Blvd., Beverly Hills, CA 90212

Spy Factory, Headquarters 4836 Whirlwind, San Antonio TX 78217
Owned and operated by an ex-DEA agent, this chain seems to be the most successful chain of spy shops in the US.
SF, 6991 Blanco Rd., San Antonio, TX 78261
SF, 3871 Roswell Rd., C-4, Atlanta, GA 30342
SF, 7619 S. Orange Blossom Trail, Orlando, FL 32809
SF, 4289 Belt Line Rd., Dallas, TX 75244
SF, 7200 W. Alameda, Denver, CO 80226
SF, 4702 E. Broadway 106, Tueson, AZ 85711
SF, 527 S. Dearborne St., Chicago, H 60605
SF, 1820 Market St., 104 St Louis, MO 63103
SF, 5358 Westheimer Houston, TX 77056
SF, 6324 Edgemere, El Pase, TX 79925
SF, 309, S. Main St., Salt Lake City, UT 841 11
SF, 2228 Paradise Rd., Las Vegas, NE 89104
SF, 10560 Magnolia Ave 3B, Riverside, CA 92505
SF, 8521 Sunset Blvd., W. Hollywood, CA 90069
SF, 3555 Rosecrans 104B, San Diego, CA 92110
SF, 1914 Harbor Blvd., Costa Mesa, CA 92627
SF, 3740 Filmore St., San Francisco, CA 94123
SF, 1401 2nd Avenue, Suite 229-A, Seattle, WA 98101

Audio Intelligence Devices, 1400 NW 62nd St., Fort Lauderdale, FL 33309
AID is the largest supplier of surveillance equipment in the U. S. They offer a diverse line of products from complete intelligence systems, including their unique UNITEL series that offers scrambled or clear voice, high band operation, rechargeable batteries, complete unattended recorder, performance to scramblers, body mikes, hardwires, through wall devices, processors, acoustic sensors, tiny transmitters, etc.

AMC Sales Inc., Dept. A, 9335 Lubee St., Box 928, Downey, CA 90241
AMC is one of the original producers of low cost surveillance equipment and specialise in phone recording adapters, VOX control switches and modified cassette recorders.

Aveom of Virginia, Inc., 500 Southlake Blvd. Richmond, VA 23236
Excellent producer of a spectrum analyser, plus other test equipment and a broadcast quality microwave transmitting system.

Bartlett Technologies Corp., 6858 NW 75th St., Bldg 3, Miami, FL 33166
Data intercept technology, loop extenders, slaves and dialled number recorders for the law enforcement community.

BH & A, 266 San Lorenzo St., Pomona, CA 91766
General consumer supplier of transcribers and portable cassette recorders at discount prices.

Capri Electronics Corp. PO Box 589, Bayfield, CO 81122
Capri is an OEM manufacturer of some inexpensive and effective countermeasures and privacy assurance devices, including microwave detectors, video camera detectors, bug detectors, countermeasure sets, etc.

Carol Products Co. Inc. 1750 Brielle Ave., Ocean, New Jersey, 07712
Carol Products is a video surveillance supplier who cleverly secretes miniature cameras in such items as smoke alarms, notebooks, sirens, etc. They also stock wide angle and pin hole lenses.

Cellular Press, 421 N. Rodeo Drive, 15318, Beverly Hills, CA 90210
Cellular software to change the ESN and NAM on various phones, plus hacker's books.

C.I.A. (Custom Interface Accessories) 2499 Lincoln Blvd., Marina del Rey, CA. 90291
Telephones, adapters, recorders, microphones, cellular phone fax, adapters, portable fax machines, some surveillance-related items.

Computer Handman, PO Box 503, Carmel, IN 46032
An interesting communications and intelligence gathering and analysis programme that has been developed to log transmissions on various receivers and scanners and includes such data as date, time, frequency and emission type.

Covert Operations International Ltd., 276 5th Avenue, Suite 1106, New York, NY 10011
Primary supplier of the CAN TRAC 360 electronic tracking system, as well as several other electronic trackers, pen registers, telephone decoders, etc.

Datametrics Inc., 2575, S. Bayshore Dr., Suite 8A, Coconut Grove, FL 33133
Computer controlled menu-driven software that will drive a receiver for autolog and autoscanning applications.

Detection Systmes, 2525 E. Thomas Rd., 16-B64, Phoenix, AX 85016
Re-sellers of Capri Electronics. Offer a good selection, plus army surplus intrusion detection and radar equipment.

Diversified Wholesale Products, PO Box 1275, Redondo Beach, CA 90278
Countermeasures equipment, handheld transceivers with microphones.

D.K. Video Inc., PO Box 63-6025, Margate, FL 33063
Low end kits for unscrambling video signals, as well as a dropout recorder or two and a cheap transmitter.

Electronic Equipment Bank, 323 Mill St., Vienna, VA 22180
Excellent prices and selection, particularly on Kenwood, Yaesu and Sony receivers/ scanners.

Elmo Co., Ltd., 70 Hyde Park Rd., New Hyde Park, NY 11040
Manufacturer of sub-miniature colour and black and white CCTV video chip cameras.

El-Tee International Inc., 205 Van Buren St., Suite 220, Herndon, VA 22070
The ETI telemonitor is among the most intelligent monitoring devices on the market today, utilising artificial intelligence that is simply boggling!

Executive Protection Products, Inc. 1834 lst St., Napa, CA 94559
Provides a wide range of surveillance equipment, including scramblers, night vision devices, countermeasure gear, drop out recorders, pin hole lenses, etc.

F & P Enterprises, PO Box 51272, Palo Alto, CA 94303
Value added reseller of drop out recorders, parabolic microphones, etc.

General Technology Corp., 6816 Washington NE, Albuquerque, NM 87109
Manufacturer of Nagra recorders

HDS, 12310 Pinecrest Rd., Reston, VA 22091
Miniature and sub-miniature video transmitters in two different bands, microwave video links, bodywires, dialled number recorder, mini-audio transmitters, etc.

ICOM America Inc., 116th Ave., N.E. Bellevue, WA 98004
Manufacturers of the largest line of general communication receivers and scanners

INCO, PO Box 3111, Burbank, CA 91508
Suppliers of the amazing disappearing paper. They also stock a variety of fake ID's, badges, books, knives and T-shirts.

Jarvis International Intelligence Inc. PO Box 690563, Tulsa, OK 74169
Supplier of countermeasures equipment, including amplifiers and spectrum analysers.

Kigre Inc., 100 Marshland Rd., Hilton Head Island, SC 29926
Night vision devices, including some unusual goggles that incorporate a folded optical path, making them extremely compact and light.

LACUE Communications Co., 132 Village St., Johnstown, PA 15902.
Handheld and mobile programmable two-way radios.

Lourou Electronics, 6158 Lemona Aven., Van Nuys, CA. 91411
In place audio surveillance systems.

Math Associates Inc., 2200 Shames Dr., Westbury NY 11590
Fibre optic systems, including laser diode fibrelink transmitters.

Metme Corp., 11754 Westline Industrial Dr., St. Louis, MO 63146
Producers of a public key scrambled telephone and fax scrambler.

New York Security Systems, Inc., 20 Industrial Dr., Middletown, NY 10940
Covert audio and video systems, including time lapse VCR'S, wireless transmitting systems, pinhole lenses and self contained camcorders.

Olympus Corp., 4 Nevada Drive, Lake Success, NY 11042
Fiberscopes and borescopes for through wall and other covert viewing and film and recording applications. Unique scopes that are camouflaged to look like part of a plant, fit inside a car radio antenna, as well as 20' fiberscopes that can be lowered from a roof to view into windows. Top of the line equipment.

Optelcom, 15930 Luanne Dr., Gaithersburg, MD 20877
Small fibre optic transmitters and receivers for video systems

Pacific Advanced Engineering, 8755 Aero Dr., San Diego, CA 92123
Broadcast quality video receivers and encrypted receivers.

Ross Engineering Inc., 7906 Hope Valley Court Adamstown MD 21710
Extensive range of countermeasures equipment

Sherwood Communications Assoc. Ltd., Box 535 Southampton, PA 18966
Complete range of video equipment.

Surveillance Technology Group, 102 Midland Ave., Port Chester, NY 10573
Unique surveillance equipment, including ashtray transmitters, through wall probes, carrier current video transmitters, etc.

SWS Security, 1300 Boyd Rd., MD 21154
Specialises in electronic tracking devices, such as bumper beepers.

Viking Electronics Inc., 1531 Industrial St., Hudson, WI 54016
Automatic routing switches so fax machines and telephones can share the same line, DTMF controllers that operate equipment via touch-tone requests and phone line simulators, etc.

Visual Methods Inc., 35 Charles St., Westwood, NJ 07675
VMI provides video equipment with an impressive inventory of straight and right angle pinhole lenses, fixed iris lenses, miniature CCD cameras, disguise camera lenses in industrial ceiling sprinklers, fibreoptic set-ups, etc.

Watee America Corp, PO Box 6686, Thousand Oaks, CA 91360
A Japanese manufacturer of sub-miniature video cameras which are incorporated in many other people's systems or sold at a considerable mark-up.

We thank you for purchasing this NIGHT SKY book and hope that you find the information it contains to be useful to you. Our aim is to publish well written information that can genuinely improve your life.

Unlike many publishers who pad out their books, at NIGHT SKY we avoid wasting words and pages and keep to the point. This enables you to read our books much faster and with greater ease, so making it easier to assimilate and benefit from the information contained.

If you have any comments or criticisms about this book, or any others that we publish, please write to us at the address below.

Night Sky Ltd
PO Box 115, St Helier JE4 8QQ

Write to us for details of our full range of publications. We will be happy to post you our latest catalogue of exciting life changing titles – free of charge!